UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/044,114	01/10/2002	Jeff B. Anderson	01545.018a	8138

7590 03/18/2005

Daniel P. McCarthy
PARSONS, BEHLE & LATIMER
201 South Main Street, Suite 1800
P.O. Box 45898
Salt Lake City, UT 84145-0898

EXAMINER	
REILLY, SEAN M	

ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/044,114	ANDERSON ET AL.	
	Examiner	Art Unit	
	Sean Reilly	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is a first action on the merits of this application. Claims 1-35 are presented for further examination.

Priority

1. The effective filing date for the subject matter defined in the pending claims in this application is 1/10/2001.

Specification

2. The abstract of the disclosure is objected to because it exceeds the 150-word limit. Correction is required. See MPEP § 608.01(b).

3. The specification is objected to for not cross-referencing co-pending applications 10/043426 and 10/044632 in the section entitled CROSS-REFERENCE TO RELATED APPLICATIONS.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-35 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-29 of copending Application No. 10/043426. Although the conflicting claims are not identical, they are not patentably distinct from each other. Refer to the tables and remarks below for specific claim mappings and further explanation.

5. Claims 1-35 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-21 of copending Application No. 10/044632. Although the conflicting claims are not identical, they are not patentably distinct from each other. Refer to the tables and remarks below for specific claim mappings and further explanation.

6. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

7. In the instant application, claim 35 substantially incorporates the limitations of independent claims 1 and 29. Similarly claim 26 of application 10/043426 substantially incorporates the

limitations of independent claims 1, 11, 20, 21, 22; and claim 17 of application 10/044114 substantially incorporates the limitations of independent claims 1, 5, 9, 10, and 11. Thus, the limitations of claim 35 in the instant application are mapped to the limitations of claim 26 application 10/043426 and claim 17 application 10/044632 to form the basis for the double patenting rejection.

8. Claim 35 of the instant application is directed to a system for remotely monitoring or controlling devices in an enterprise, while claim 26 of co-pending application 10/043426 is directed to a method for accessing such a system. The system of claim 35 must be used to execute the method of claim 26, since claim 26 claims the same system structure as claim 35 of the instant application, thus co-pending claim 26 is not patentably distinct. Regarding co-pending application 10/044632, claim 17 of the co-pending application is directed to a substantially identical system as claimed in claim 35 of the instant application and is therefore not patentably distinct. Refer to the claim mappings below for further explanation.

Co-pending Application # 10/043426 Claim 26	Instant Application # 10/044114 Claim 35
26. A method for remotely accessing and viewing information about an enterprise, comprising the steps of:	35. A reporting and maintenance system for remotely monitoring or controlling devices in an enterprise, comprising:
accessing a transferential system that has the following characteristics:	

a server group including at least two servers, said servers providing redundancy of operation, at least one non-volatile memory device incorporated to said server group,	a server group including at least two servers, said servers providing redundancy of operation; at least one non-volatile memory device incorporated to said server group;
server network hardware connected to said server group, said server network hardware including a gateway, said server network hardware being configurable to provide encrypted electronic communication between said server group and a superintendent system through said gateway, said server network hardware being further configurable to provide electronic communication between said server group and at least one enterprise device in communicative proximity,	server network hardware connected to said server group, said server network hardware including a gateway, said server network hardware being configurable to provide encrypted electronic communication between said server group and a superintendent system through said gateway, said server network hardware being further configurable to provide electronic communication between said server group and at least one enterprise device in communicative proximity;
1-10 computer readable instructions	1-10 computer readable instructions

a cabinet housing said server group, a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet, a second network enabled temperature sensor, said second temperature sensor positioned to monitor the temperature of the air outside said cabinet, at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position, locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a superintendent system, a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device, a network enabled camera whereby a space in proximity to said server group may be monitored, an alarm in proximity to said server group, a network enabled power controller connected to and being configurable to control	a cabinet housing said server group; a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet; a second network enabled temperature sensor, said second temperature sensor positioned to monitor the temperature of the air outside said cabinet; at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a superintendent system; a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device; a network enabled camera whereby a space in proximity to said server group may be monitored; an alarm in proximity to said server group; a network enabled power controller connected to and being configurable to control

Co-pending Application # 10/044632 Claim 17	Instant Application # 10/044114 Claim 35
17. A transferential system for remotely monitoring or controlling devices in an enterprise, comprising:	35. A reporting and maintenance system for remotely monitoring or controlling devices in an enterprise, comprising:
a server group including at least two servers, said servers providing redundancy of operation; at least one non-volatile memory device incorporated to said server group;	a server group including at least two servers, said servers providing redundancy of operation; at least one non-volatile memory device incorporated to said server group;
a central information system in electronic communication with said server group through said server network hardware;	See the limitation a superintendent system below.
enterprise devices in electronic communication with said server group through said server network hardware;	See the limitation at least one enterprise device below.
server network hardware connected to said server group, said server network hardware including a gateway, said server network hardware providing encrypted electronic communication between said server group and	server network hardware connected to said server group, said server network hardware including a gateway, said server network hardware being configurable to provide encrypted electronic communication between

said central information system through said gateway, said server network hardware further providing electronic communication between said server group and said enterprise devices;	said server group and a superintendent system through said gateway, said server network hardware being further configurable to provide electronic communication between said server group and at least one enterprise device in communicative proximity;
at least one notification device connected to and controllable by said central information system whereby an administrator may be notified of enterprise status; at least one display device connected to said central information system providing display facilities to administrators;	Superintendent system monitor displaying received messages (instructions 1-3 show the message transfer).
1-10 computer readable instructions	1-10 computer readable instructions
a cabinet housing said server group; a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet; a second network enabled temperature sensor, said second temperature sensor positioned to monitor the temperature of the air outside said cabinet; at least one door included	a cabinet housing said server group; a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet; a second network enabled temperature sensor, said second temperature sensor positioned to monitor the temperature of the air outside said cabinet; at least one door included

in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a central information system; a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device; an alarm in proximity to said server group; a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands from a central information system;	in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a superintendent system; a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device; a network enabled camera whereby a space in proximity to said server group may be monitored; an alarm in proximity to said server group; a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands from a superintendent system;

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1, 4-9, 19-25, 27, and 29-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Barker et al. (U.S. Patent Number 6,363,421; hereinafter Barker).

10. Regarding claims 1, 4-9, 19-25, 27, and 29-34, Barker discloses a reporting and maintenance system for remotely monitoring or controlling devices in an enterprise, the devices communicating in at least one enterprise management protocol, said reporting and maintenance system for remotely monitoring or controlling devices in an enterprise comprising:

- a server group including at least one server (Figure 2, Element Management System Server);
- at least one non-volatile memory device incorporated to said server group (inherent);
- enterprise devices in electronic communication with said server group through said server network hardware (Figure 2, Network Element);
- a central information system (or superintendent system) in electronic communication with said server group through said server network hardware (Figure 2, Element Management System Client);

- server network hardware connected to said server group, said server network hardware including a gateway (inherent for network connection communication, see connections in Figure 3),
- said server network hardware providing encrypted electronic communication between said server group and said central information system through said gateway (Col 8, lines 45-49), said server network hardware further providing electronic communication between said server group and said enterprise devices (Figure 3, network connections);
- first computer readable instructions installed to said memory devices, said first instructions providing the function of receiving first messages from enterprise devices in at least one enterprise management protocol including version 1 of SNMP (Traps), said first computer readable instructions providing a message gateway (SNMP Mediator) (Col 21, lines 25-27);
- second computer readable instructions installed to said memory devices, said second instructions providing the function of forwarding the information contained in the first messages to a central information system by a notification channel (Col 17, lines 5-18).
- third computer readable instructions installed to said memory devices, said third instructions providing the function of filtering the first messages, the filtering preventing the forwarding of some of the first messages, said filtering prescribed by policy (filter) (Col 17, lines 5-18);

- fourth computer readable instructions installed to said memory devices, said instructions providing the function of translating the first received messages to a second protocol, said first, second, third, fourth, and fifth computer readable instructions providing an event translator (Col 21, lines 31-32);

The following instructions (6-8) relate to a client issuing a command. (i.e. a command from the central information system routed through the server group to an enterprise device. See example (Col 22, line 46 –Col 23, line 6) and the references below.

- sixth computer readable instructions installed to said memory devices, said instructions providing the function of receiving second messages from a central information system through a notification channel, said second messages referencing at least one enterprise device (Col 22, lines 49-59);
- seventh computer readable instructions installed to said memory devices, said instructions providing the function of translating the second received messages to an enterprise management protocol utilized by the referenced enterprise devices (Col 19, lines 13-23);
- eighth computer readable instructions installed to said memory devices, said instructions providing the function of forwarding the information in the second messages to the referenced enterprise devices in at least one enterprise management protocol including version 1 of the simple network management protocol (Col 22, lines 64-67) or (Col 19, lines 55-60),

- said sixth, seventh, and eighth computer readable instructions providing an SNMP translator (Col 19, lines 13-23);
- said tenth instructions providing the function of receiving a software upgrade from a central information system, said tenth instructions also providing the function of delivering the software upgrade to enterprise devices (Col 30, lines 1-25).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker et al. (U.S. Patent Number 6,363,421; hereinafter Barker).

12. Regarding claims 2 and 3, Barker discloses a forwarder for forwarding the information contained in the first messages (Col 17, lines 5-18). Barker fails to disclose sending the messages in a preferential order by an assigned priority from the server group to the central information server. However, Barker does disclose that enterprise devices send traps to the server group in a preferential order by an assigned priority using high and low priority queues (i.e. command acks being high priority and information messages being low priority) so the server group is not overwhelmed, a form of overload control (Col 34, lines 51-60). Barker further discloses that client (central information servers) overload may be a problem so overload controls should be implemented to restrict client overload (Col 29, lines 41-53). Thus, it would

have been obvious to one of ordinary skill in the in the art at the time of the invention to implement the enterprise device overload controls within the server group, in order to prevent the central information server from being overloaded with messages.

13. Claims 10-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker et al. (U.S. Patent Number 6,363,421; hereinafter Barker) in further view of Fowler et al. (U.S. Patent Number 6,714,977) and the knowledge of one of ordinary skill in the art.

14. Regarding claims 10-18, Barker fails to disclose the following:

- a cabinet housing said server group;
- a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet; a second network enabled temperature sensor, said second temperature sensor positioned to monitor the temperature of the air outside said cabinet;
- at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a central information system;
- a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device;
- an alarm in proximity to said server group;

- a network enabled camera whereby a space in proximity to said server group may be monitored
- a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands from a central information system;

Nevertheless, such physical computer room equipment and monitoring mechanisms were well known in the art at the time of the invention, as evidenced by Fowler. In a related art, a method for monitoring computer networks and equipment (abstract). Fowler discloses a cabinet housing a server group (rack, Figure 1, Component 12). Fowler further discloses monitoring the air temperature (Col 7, lines 11-13), an alarm (Col 7, lines 26-27), a camera (Col 7, lines 29-33) and a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands from a central information system (Col 10, lines 38-41). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the network monitoring devices disclosed by Fowler within the Barker system, in order to alert network administrators to out of limit environmental variables which damage computer equipment (Fowler Col 2, lines 38-40).

Although Fowler fails to disclose at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a central information system; the importance of

physically securing computer systems was well known in the art at the time of the invention as disclosed by Fowler (Fowler Col 2, lines 30-31). Further, the Examiner takes official notice that doors containing locally/remotely controllable locks were well known in the art at the time of the invention. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to use industry standard security measures such as placing a door with a locally/remotely controllable lock on the rack disclosed by Fowler, in order to further secure the sever components.

15. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Barker et al. (U.S. Patent Number 6,363,421; hereinafter Barker) as applied above and in further view of Sampson ("Unicenter TNG for Dummies").

16. Regarding claim 26, Barker fails to disclose instructions installed to said memory devices, providing the function of accepting network parameters that define the boundaries of an enterprise, also providing the function of discovering enterprise devices through said server network hardware using the network parameters. In a related art, Sampson discloses an enterprise management system which provides the function of accepting network parameters that define the boundaries of an enterprise, and discover enterprise devices through said server network hardware using the network parameters (Sampson pg 22-23). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Sampson's enterprise discovery functionality within Barker system in order to automate the entry and management of enterprise devices (Sampson pg 22).

17. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Barker et al. (U.S. Patent Number 6,363,421; hereinafter Barker) and Examiner's Official Notice.

18. Regarding claim 28, the Examiner takes official notice that it was well known in the art at the time of the invention to use multiple servers in a redundant fashion in order to maintain network sustainability for clients. It would have been obvious to one of ordinary skill in the art at the time of the invention to use redundant servers in the Barker system in order to maintain network sustainability for clients.

19. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Barker et al. (U.S. Patent Number 6,363,421; hereinafter Barker) and Fowler et al. (U.S. Patent Number 6,714,977); hereinafter Fowler) and Sampson ("Unicenter TNG for Dummies") and the knowledge of one of ordinary skill in the art at the time of the invention.

20. Regarding claim 35, Barker discloses a transferential system for remotely monitoring or controlling devices in an enterprise, comprising:

- a server group including at least one server (Figure 2, Element Management System Server);
- at least one non-volatile memory device incorporated to said server group (inherent);
- enterprise devices in electronic communication with said server group through said server network hardware (Figure 2, Network Element);
- a central information system in electronic communication with said server group through said server network hardware (Figure 2, Element Management System Client);

- server network hardware connected to said server group, said server network hardware including a gateway (inherent for network connection communication, see connections in Figure 3),
- said server network hardware providing encrypted electronic communication between said server group and said central information system through said gateway (Col 8, lines 45-49), said server network hardware further providing electronic communication between said server group and said enterprise devices (Figure 3, network connections);
- first computer readable instructions installed to said memory devices, said first instructions providing the function of receiving first messages from enterprise devices in at least one enterprise management protocol including version 1 of SNMP (Traps), said first computer readable instructions providing a message gateway (SNMP Mediator) (Col 21, lines 25-27);
- second computer readable instructions installed to said memory devices, said second instructions providing the function of forwarding the information contained in the first messages to a central information system by a notification channel (Col 17, lines 5-18). Barker fails to disclose sending the messages in a preferential order by an assigned priority from the server group to the central information server. However, Barker does disclose that enterprise devices send traps to the server group in a preferential order by an assigned priority so the server group is not overwhelmed, a form of overload control (Col 34, lines 51-60). Barker further discloses that client (central information servers) overload may be a problem so overload controls should

be implemented to restrict client overload (Col 29, lines 41-53). Thus, it would have been obvious to one of ordinary skill in the in the art at the time of the invention to implement the enterprise device overload controls within the server group, in order to prevent the central information server from being overloaded with messages.

- third computer readable instructions installed to said memory devices, said third instructions providing the function of filtering the first messages, the filtering preventing the forwarding of some of the first messages, said filtering prescribed by policy (filter) (Col 17, lines 5-18);
- fourth computer readable instructions installed to said memory devices, said fourth instructions providing the function of assigning priority to the information in said first messages (Col 34, lines 51-60);
- fifth computer readable instructions installed to said memory devices, said instructions providing the function of translating the first received messages to a second protocol, said first, second, third, fourth, and fifth computer readable instructions providing an event translator (Col 21, lines 31-32);

The following instructions (6-8) relate to a client issuing a command. (i.e. a command from the central information system routed through the server group to an enterprise device. See example (Col 22, line 46 –Col 23, line 6) and the references below.

- sixth computer readable instructions installed to said memory devices, said instructions providing the function of receiving second messages from a central

information system through a notification channel, said second messages referencing at least one enterprise device (Col 22, lines 49-59);

- seventh computer readable instructions installed to said memory devices, said instructions providing the function of translating the second received messages to an enterprise management protocol utilized by the referenced enterprise devices (Col 19, lines 13-23);
- eighth computer readable instructions installed to said memory devices, said instructions providing the function of forwarding the information in the second messages to the referenced enterprise devices in at least one enterprise management protocol including version 1 of the simple network management protocol (Col 22, lines 64-67) or (Col 19, lines 55-60),
- said sixth, seventh, and eighth computer readable instructions providing an SNMP translator (Col 19, lines 13-23);
- said tenth instructions providing the function of receiving a software upgrade from a central information system, said tenth instructions also providing the function of delivering the software upgrade to enterprise devices (Col 30, lines 1-25).

Barker fails to disclose the following:

- a cabinet housing said server group;
- a first network enabled temperature sensor, said first temperature sensor positioned to monitor the temperature of the air at the interior of said cabinet; a second network

enabled temperature sensor, said second temperature sensor positioned to monitor the temperature of the air outside said cabinet;

- at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a central information system;
- a data entry device connected to said locks, said data entry device being mounted to said cabinet, said data entry device providing a human interface external to the cabinet enclosure; said locks enabled to be unlocked through said data entry device;
- an alarm in proximity to said server group;
- a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands from a central information system;

Nevertheless, such physical computer room equipment and monitoring mechanisms were well known in the art at the time of the invention, as evidenced by Fowler. In a related art, a method for monitoring computer networks and equipment (abstract). Fowler discloses a cabinet housing a server group (rack, Figure 1, Component 12). Fowler further discloses monitoring the air temperature (Col 7, lines 11-13), an alarm (Col 7, lines 26-27), a camera (Col 7, lines 29-33) and a network enabled power controller connected to and being configurable to control the power of at least one server of said server group, said power controller being configurable to accept network commands from a central information system (Col 10, lines 38-41). It would

have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the network monitoring devices disclosed by Fowler within the Barker system, in order to alert network administrators to out of limit environmental variables which damage computer equipment (Fowler Col 2, lines 38-40).

Although Fowler fails to disclose at least one door included in said cabinet whereby access to said server group is restricted when said doors are in closed position; locks included in said doors whereby said doors may be secured in a closed position, said locks enabled to unlock through an electronic command message from a central information system; the importance of physically securing computer systems was well known in the art at the time of the invention as disclosed by Fowler (Fowler Col 2, lines 30-31). Further, the Examiner takes official notice that doors containing locally/remotely controllable locks were well known in the art at the time of the invention. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to use industry standard security measures such as placing a door with a locally/remotely controllable lock on the rack disclosed by Fowler, in order to further secure the sever components.

Barker fails to disclose ninth computer readable instructions installed to said memory devices, said ninth instructions providing the function of accepting network parameters that define the boundaries of an enterprise, said ninth instructions also providing the function of discovering enterprise devices through said server network hardware using the network parameters. In a related art, Sampson discloses an enterprise management system which provides the function of accepting network parameters that define the boundaries of an enterprise, and discover enterprise devices through said server network hardware using the

network parameters (Sampson pg 22-23). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Sampson's enterprise discovery functionality within Barker system in order to automate the entry and management of enterprise devices (Sampson pg 22).

Regarding the limitation at least two servers providing redundancy of operation, the Examiner takes official notice that it was well known in the art at the time of the invention to use multiple servers in a redundant fashion in order to maintain network sustainability for clients. It would have been obvious to one of ordinary skill in the art at the time of the invention to use redundant servers in the Barker system in order to maintain network sustainability for clients.

Conclusion

21. The prior art made of record, in PTO-892 form, and not relied upon is considered pertinent to applicant's disclosure.

22. This office action is made **NON-FINAL.**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sean Reilly whose telephone number is 571-272-4228. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess can be reached on 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

3/8/2005

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100